REMARKS

This is in response to the Office Action dated October 27, 2009. In view of the above amendments and the following remarks, reconsideration of the rejection and further examination are requested.

Rejection under 35 U.S.C §101:

Claims 37-38 and 41 have been rejected under 35 U.S.C §101 as being directed to non-statutory subject matter. This rejection is submitted to be inapplicable to the claims for the following reasons.

Claims 37-38 and 41 have been cancelled without prejudice or disclaimer to the subject matter therein.

Rejection under 35 U.S.C §102(b):

Claims 1-42 have been rejected under 35 U.S.C §102(b) as being anticipated by Asano (US 7,088,822). Claims 37-38 and 41 have been cancelled. This rejection is submitted to be inapplicable to the claims, as amended, for the following reasons.

Claim 1 recites, in part, a first association unit operable to search, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and to associate the another subset as an association source with the subset as an association destination, a second association unit operable to search for another subset that wholly contains the containing subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and to associate the subset as a new association source with the another subset as a new association destination, a first assignment unit operable to bring pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer, and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer, and a second assignment unit operable to bring, for

a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of new unique information.

Using the above structure as recited in claim 1, it is possible to associate, in two sub-trees whose roots are respectively a parent node and a child node in a parent-child relationship, a subset F1 in a plurality of subsets generated in a sub-tree whose root is the child node with a subset F2 including the subset F1 in a plurality of subsets generated in a sub-tree whose root is the parent node. This makes it possible to associate subsets from two different sub-trees with each other (i.e., associate different sub-trees with each other), thereby decreasing the number of unique pieces of information that need to be distributed and maintained in the system. Asano fails to disclose or suggest the above features as recited in claim 1.

Asano discloses a technique for performing key management by means of a tree structure. In the key management of Asano, each leaf in the tree structure is assigned to a playback apparatus, and each node is assigned to a key. Since the keys do not depend on one another, <u>it is necessary for the playback apparatus to manage all of the keys existing in all paths from the root to the apparatus</u>. For example, Asano discloses that a device 0 would possess leaf key K0000 and node keys K000, K00, K0, and KR (see col. 20, lines 12-20). This method results in a complicated tree structure, which causes an increase in the number of playback apparatuses that manage the keys and an increase in the number of keys assigned to each playback apparatus. However, Asano does not disclose associating the subset F1, belonging to the lowermost layer, with the subset F2, belonging to an immediately upper layer.

Asano also discloses the relations among the indexes 0, 00, 000 and that keys assigned to the indexes 00, 0 are obtained from encrypted data corresponding to the index 000 one by one, as shown in Figure 12 (see col. 21, lines 25-49). However, Asano does not disclose assigning new pieces of unique information obtained from pieces of unique information assigned to a subset

belonging to one of the layers, to another subset with which the subset is associated. This means that the assignment of pieces of unique information is performed between two subsets between one layer and an immediately upper layer.

Therefore, Asano does not disclose or suggest a first association unit operable to search, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and to associate the another subset as an association source with the subset as an association destination, a second association unit operable to search for another subset that wholly contains the containing subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and to associate the subset as a new association source with the another subset as a new association destination, a first assignment unit operable to bring pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer, and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer, and a second assignment unit operable to bring, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of new unique information, as recited in claim 1. As a result, claim 1 is not anticipated by Asano.

Claim 25 is not anticipated by Asano for the same reasons as those discussed above with regard to independent claim 1. Specifically, claim 25 recites a first association unit operable to search, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof,

and to associate the another subset as an association source with the subset as an association destination, a second association unit operable to search for another subset that wholly contains the subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and to associate the subset as a new association source with the another subset as a new association destination, a first assignment unit operable to bring pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer, and to assign each piece of unique information to apparatus identifiers contained in the respective subset in the lowermost layer, and a second assignment unit operable to bring, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of new unique information. Since the above features, as recited in claim 25, are not disclosed or suggested by Asano, it is submitted that claim 25 is not anticipated by Asano.

Claims 40 and 42 are not anticipated by Asano for reasons similar to those discussed above with regard to independent claim 1. Specifically, claims 40 and 42 recite a first association step of searching, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and associating the another subset as an association source with the subset as an association destination, a second association step of searching for another subset that wholly contains the subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and to associate the subset as a new association source with the another subset as a

27

new association destination, a first assignment step of bringing pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer, and assigning each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer, and a second assignment step of bringing for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations and assigning the pieces of new unique information to apparatus identifiers contained in the one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of new unique information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of new unique information. Since the above features, as recited in claims 40 and 42, are not disclosed or suggested by Asano, it is submitted that claims 40 and 42 are not anticipated by Asano.

Claim 14 is not anticipated by Asano for reasons similar to those discussed above with regard to independent claim 1. Specifically, claim 14 recites a management apparatus that searches, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof, and performs a first association for associating the another subset as an association source with the subset as an association destination, searches for another subset that wholly contains the containing subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediately upper layer thereof and generated by the subset generating unit for a parent node of the node, and performs a second association for associating the subset as a new association source with the another subset as a new association destination, performs a first assignment for bringing pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in lowermost layer, and performs a second assignment for bringing, for a subset being an association source generated for a node in one of layers and one or more subsets being association destinations

positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of new unique information into correspondence respectively with the one or more subsets being association destinations, and to assign the pieces of new unique information to apparatus identifiers contained in one or more subsets being association destinations, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of new unique information. Since the above features, as recited in claim 14, is not disclosed or suggested by Asano, it is submitted that claim 14 is not anticipated by Asano.

Claim 39 is not anticipated by Asano for reasons similar to those discussed above with regard to independent claim 1. Specifically, claim 39 recites an integrating unit operable to, after the second control unit performs the processing on all of the layers, integrate into one group (i) a lower-layer group and (ii) an upper-layer group that includes a subset that wholly contains one of subsets belonging to the lower-layer group and that is generated for a parent node of a node for which the one of subsets are generated, the lower-layer group and the upper-layer group belonging to mutually different layers, and a second assignment unit operable to bring pieces of new unique information into correspondence with subsets other than the subset that has the smallest number of elements respectively and assigns each piece of new unique information to one or more apparatus identifiers that are contained in each of said other subsets, the pieces of new unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset that has the smallest number of elements respectively to generate corresponding decryption keys and pieces of new unique information. Similarly to claim 1, the above features, as recited in claim 39, make it is possible to associate, in two sub-trees whose roots are respectively a parent node and a child node in a parent-child relationship, a subset (Fl) in a plurality of subsets (subset differences) generated in a sub-tree whose root is the child node with a subset (F2) including the subset FI in a plurality of subsets generated in a sub-tree whose root is the parent node. This makes it possible to associate subsets included in two different sub-trees with each other, that is, to associate different sub-trees with each other, thereby decreasing the number of the unique information pieces to be distributed.

As noted above, Asano does not disclose the association of a subset (Fl) in a plurality

of subsets generated in a sub-tree whose root is the child node with a subset F2 including the subset F1 in a plurality of subsets generated in a sub-tree whose root is the parent node. Therefore, claim 39 is not anticipated by Asano.

Claims 2-13 are either directly or indirectly dependent on independent claim 1. Claims 15-24 are either directly or indirectly dependent on independent claim 14. Claims 26-36 are either directly or indirectly dependent on independent claim 25. As a result, claims 1-36, 39-40, and 42 are allowable over Asano.

Because of the above-mentioned distinctions, it is believed clear that claims 1-36, 39-40, and 42 are allowable over the reference relied upon in the rejection. Furthermore, it is submitted that these distinctions are such that they would not have been obvious to a person having ordinary skill in the art at the time of the invention. Therefore, it is submitted that claims 1-36, 39-40, and 42 are clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The examiner is invited to contact the undersigned by telephone if it is felt that there are issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Toshihisa NAKANO et al.

/Allen N. Doyel/
By 2010.01.26 14:17:37 -05'00'
Allen N. Doyel
Registration No. 60,391
Attorney for Applicants

AND/MSH/clw
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 27, 2010